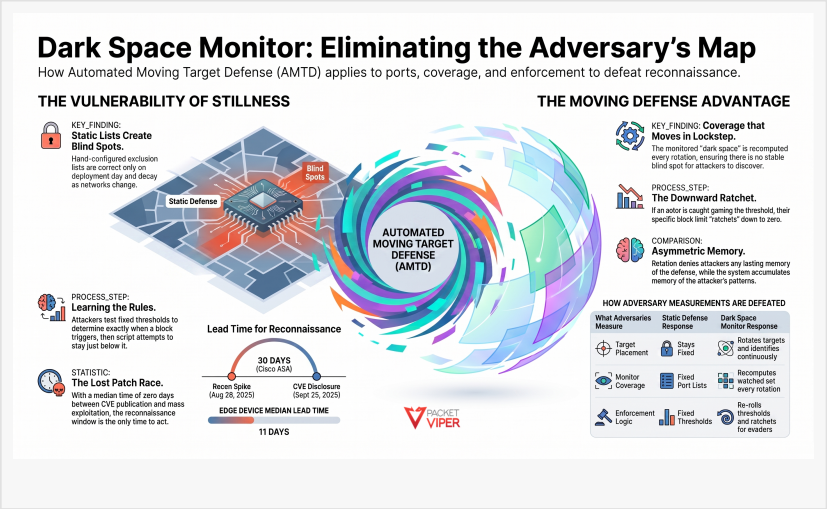
PacketViper Introduces Dark Space Monitor, Bringing Automated Moving Target Defense to Every Port an Adversary Probes

PITTSBURGH, PA, UNITED STATES, August 7, 2026 /EINPresswire.com/ -- PacketViper today introduced Dark Space Monitor, the capability that delivers dark space monitoring, detection, and prevention within its Automated Moving Target Defense platform. It is built for the phase of an attack that most defenses never see: the reconnaissance that happens before anything is exploited.



As federal agencies warn of Iranian-affiliated actors exploiting internet-exposed controllers at U.S. water and energy utilities, PacketViper's Dark Space Monitor watches the ports where nothing is presented, moves that coverage on every rotation, and turns an attacker's evasion of the block threshold into their own exposure.

Automated Moving Target Defense is the doctrine of defeating reconnaissance by continuously changing the attack surface an adversary observes. Dark space is attack surface. The ports where nothing is presented are as much a part of what an attacker maps as the ports where something is, and watching them has always been part of what the doctrine requires — a defense defined by what an adversary observes cannot exclude the places where it presents nothing. Dark Space Monitor is how PacketViper delivers that. The phase it targets is now measurable, and the measurements are not comfortable reading for defenders.

In April 2026, the FBI, CISA, NSA, EPA, the Department of Energy, U.S. Cyber Command, and the Department of the Treasury issued joint advisory AA26-097A warning that Iranian-affiliated actors were exploiting internet-exposed programmable logic controllers across U.S. water, energy, and government infrastructure. In July 2026 the agencies updated that advisory to widen the targeted equipment beyond Rockwell Automation to include Schneider Electric and Siemens controllers. The advisory's central mitigation is to remove those controllers from direct internet exposure. That is sound guidance, and it addresses the devices an operator knows are exposed.

It does not address the ports an operator was never watching.

The scale of that unwatched surface is substantial. Bitsight research published in June 2026 tracked roughly 170,000 internet-exposed industrial control and operational technology devices per month across fifteen protocols through 2025. Every one of those environments has ports where nothing is presented and, in most deployments, nothing is watching.

Reconnaissance is not noise. It is the warning.

New research quantifies how reliably scanning precedes exploitation. In an April 2026 report analyzing 147.8 million sessions over 103 days across 276 detection signatures spanning eighteen edge-device and network-infrastructure vendors, GreyNoise found that more than half of the activity surges it identified were followed by a vendor-matched CVE disclosure within three weeks. The median lead time was eleven days.

The pattern has already played out publicly. On August 26, 2025, GreyNoise observed more than 25,000 unique IP addresses scanning the Cisco ASA web login path in a single burst, against a normal baseline of fewer than 500 addresses per day. GreyNoise published the anomaly on September 4, 2025, and stated plainly that it could indicate an upcoming Cisco ASA vulnerability disclosure. On September 25, Cisco disclosed two actively exploited zero-day vulnerabilities in that platform. The scanning was visible three weeks before the vulnerability was public.

Verizon's 2025 Data Breach Investigations Report found that for edge-device vulnerabilities, the median time between CVE publication and mass exploitation is zero days, while median time to full remediation is 32 days. Once a vulnerability is public, the patch race is already lost. The reconnaissance window beforehand is the interval defenders can still act inside — if they can see it.

Everything an adversary can measure.

Moving target defense works because an attacker cannot build a stable map. PacketViper rotates the addresses, ports, and presented identities an adversary sees, so reconnaissance gathered minutes ago is already wrong. The principle governs everything an adversary can measure about the defense — not only where targets are presented, but where the appliance watches and when it enforces.

Adversaries work all three. An attacker who fingerprints which ports are presenting targets does the obvious thing next: they probe the ports that are not. Where that coverage is defined by a port list entered once during installation, it can be found and it stays found. A fixed enforcement threshold is likewise a rule, and rules are learnable: an attacker who determines that the fifth attempt triggers a block instructs their tooling to stop at four, change source address, and begin again. Against a static counter, it never trips, enforcement never fires, and nothing appears on the operator's console — precisely the outcome the adversary engineered.

Dark Space Monitor answers both the same way PacketViper answers placement. It watches dark space, defined as the complement of the currently active targets: every port where PacketViper is presenting nothing. Because nothing legitimate has any reason to reach into that space, every hit is meaningful and falls into one of three categories that all warrant attention: a misconfigured device, an undocumented setting, or a threat scanning around the targets it has already fingerprinted.

Critically, the watched set is recomputed in the same action as the rotation rather than by a separate process attempting to keep pace. The monitor never watches a port that is actively presenting a target, and never leaves a just-vacated port uncovered. There is no interval for an adversary to slip through, and no fixed gap to discover.

Enforcement follows the same principle. The block threshold is re-rolled within a configured band on every rotation, so a threshold measured on one cycle is invalid on the next. When a source repeatedly stops just short of the limit and hands off to a fresh address against the same target, that signature is recognized as deliberate evasion, and the effective threshold for that actor ratchets downward until they are caught on the first attempt. The adversary's own evasion drives their exposure.

"Dark space has always been part of what moving target defense has to cover, because it is part of what the attacker is measuring," said Francesco Trama, CEO and Founder of PacketViper. "The ports where you answer nothing tell a scanner as much as the ports where you answer something, and so does the moment you decide to block. If any of that sits still, you have handed the attacker a fixed reference point, and a competent one will find it. The industry has also trained operators to treat scanning as background noise, and the data now says the opposite. When researchers can watch a scanning spike and call the vulnerability three weeks before the vendor announces it, that reconnaissance was never noise. It was the warning. Rotation denies the attacker any lasting memory of us, and the pattern-watcher gives us accumulating memory of them. We remember them, and they cannot remember us."

Built for environments that cannot be taken offline.

Because the targets in this context are presented by PacketViper rather than production systems, the threshold can safely be driven to zero. Nothing legitimate ever communicates with them, so there is no live service to disrupt and no collateral impact on a production device. That scoping is deliberate and is not relaxed elsewhere: PacketViper's surgical enforcement principle, which scopes action to the specific device and never to the subnet, continues to govern rules protecting real assets.

This matters in operational technology, where the equipment named in AA26-097A frequently cannot be patched, cannot run an agent, and cannot be taken out of service for a maintenance window. Dragos, in its 2026 OT Cybersecurity Year in Review, reported that only 46 percent of its

customer assessments found adequate OT network monitoring in place, and that 81 percent found poor segmentation between IT and OT networks. In environments with those gaps, a capability that requires no agent, no device reconfiguration, and no port list is the difference between coverage and none.

Operators may also choose an intelligence-optimized posture. Rather than blocking on first contact, a non-zero threshold permits a brief, controlled window while the adversary believes they are successfully staying under the limit. During that window PacketViper captures the credentials attempted, the attack sequence, and attribution of the tooling in use. Enforcement then fires on the defender's timing rather than the attacker's. The window always terminates in enforcement.

Consistent with PacketViper's approach to operational technology, the capability can be run in observation mode first, surfacing everything reaching dark space without enforcing, so operators understand their environment before narrowing in. Detected evasion behavior and enforcement state are presented to the operator rather than acted on silently, keeping the human in control of posture.

Dark Space Monitor requires no port lists and no ongoing exclusion maintenance. A hand-built exclusion list is accurate the day it is written and decays from that point forward; a set derived from the rotation is accurate continuously. Configuration is a single toggle and a choice of action: block, log, or alert.
The capability is managed centrally through PacketViper's Federation Manager, so posture is applied consistently across a distributed footprint with no gap and no bypass path. Dark Space Monitor runs alongside command-level OT protocol protection, network sensors, and federation on the same single agentless appliance. What competitors require several products to accomplish, PacketViper delivers on one. Because every dark-space event and enforcement action is recorded, the audit trail is a byproduct of normal operation rather than a separate reporting exercise.

About PacketViper
PacketViper is an Automated Moving Target Defense company that protects operational technology and critical infrastructure with preemptive, agentless, inline enforcement on a single appliance. PacketViper is U.S.-owned and U.S.-staffed with no foreign ownership, control, or influence, and is available on the GSA Schedule and Army CHESS ITES-SW2. To learn more, visit www.packetviper.com.

Sources:
The following public advisories and industry reports provide background for the cybersecurity trends and threat activity discussed in this announcement.

CISA, FBI, NSA, EPA, DOE, U.S. Cyber Command, and U.S. Department of the Treasury
AA26-097A: Iranian-affiliated cyber actors exploiting internet-exposed programmable logic

controllers (Updated July 22, 2026)
https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

Bitsight
2026 Global State of ICS/OT Exposure (June 4, 2026)
https://www.bitsight.com/blog/2026-global-state-of-ics-ot-exposure

GreyNoise Intelligence
Ten Days Before Zero: How Cyber Threat Activity Precedes Vulnerability Disclosure (April 20, 2026)
https://www.greynoise.io/press/report-how-cyber-threat-activity-precedes-vulnerability-disclosure

GreyNoise Intelligence
Scanning Surge Targeting Cisco ASA Devices Could Indicate Upcoming Vulnerability Disclosure (September 4, 2025; updated September 26, 2025)
https://www.greynoise.io/blog/scanning-surge-cisco-asa-devices

Verizon
2025 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf

Dragos
2026 OT Cybersecurity Year in Review (February 17, 2026)
https://www.dragos.com/blog/dragos-2026-ot-cybersecurity-year-in-review

Tim Jencka
PacketViper
+1 412-212-6348
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/932222706

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.